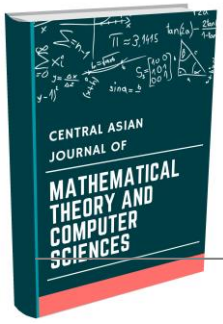

CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES

https://cajmtcs.centralasianstudies.org

Volume: 04 Issue: 8 | Aug 2023 ISSN: 2660-5309

MODELS, ALGORITHMS AND SOFTWARE FOR IDENTIFYING MALICIOUS INFORMATION IN SOCIAL NETWORKS

Mallayev Oybek Usmankulovich

Head of the Department of Digital Technologies of Perfect University

Mirzaeva Malika Bakhadirovna

Associate Professor of the department "Hardware and software of management systems in telecommunications"

A. O. Mukhamedaminov

UNICON.UZ SHOP, Standardization base organization engineer

Abstract

In this article, the opinions and comments of our country's and foreign scientists are mentioned about the improvement of models, algorithms and software complex for identifying harmful information in social networks.

ARTICLEINFO

Article history:
Received 3 Jun 2023
Revised form 5 Jul 2023
Accepted 23 Aug 2023

Keywords: *information security, cyberattack, cybercrime, algorithm, virus, antivirus.*

INTRODUCTION

The development of information technologies in Uzbekistan and their implementation in all areas of society includes the introduction of information security systems. This is because with the advent of modern technologies, various threats are rapidly developing in the virtual environment. And existing information security technologies are becoming obsolete. In the last few years, this phenomenon has become more noticeable. "A cybercriminal's primary desire is to profit from the execution of threats, and the more opportunities technology creates, the more opportunities they (cybercriminals) have to accomplish their goals." In recent years, information security in the Republic of Uzbekistan has been implemented in the following directions. This is:

1. Improvement and development of the regulatory framework.

2. Development and implementation of information security software.

International exposure and exchange of best practices with other countries. Despite the above, issues of development and coordination of necessary measures in the field of information security are still relevant.

Information and psychological security are processes and measures carried out by the state, society and private individuals, accompanying information technologies everywhere, up to the point of complete integration with them in one place.

Cyberbullying is an attack aimed at inflicting psychological harm, which is carried out through various communication platforms: e-mail, instant messaging services, chat rooms, social networks, websites, as well as mobile communication and the Internet. If organizations with good information security professionals on staff have any protection, the average user of data networks is the most vulnerable link in the security process.

Often they are victims of trolling, cachenism or various types of cyber attacks. Unfortunately, an ordinary user who does not have special knowledge or any computer skills becomes a defenseless victim of Internet information security threats. Therefore, it is not surprising that they often become victims of cybercriminals. Even if the attack is targeted at the organization, the user is still a victim.

METHODOLOGY

Analysis of the structure of social networks in information and communication systems. A social network is a structure consisting of a set of nodes (users, groups or communities) and connections between them (social interactions) that can be represented as a graph $G = (V, E)$.

Social networks can be divided into the following groups according to their architecture:

Partially decentralized (hybrid) solutions. One example is the Diaspora social network, which consists of many interconnected nodes, each of which is a separate web server. The social network has a client-server architecture, users can choose which server to connect to.

Fully decentralized P2P (peer-to-peer) social networks . Data is stored and processed by the client, which is also the server. These social networks include: LifeSocial, PeerSoN, Safebook, Pandora.

Thus, we can conclude that if it is necessary to stop the spread of malicious information in social networks, several nodes where the spread and interaction of users are carried out without the need to completely block the entire social network enough to block.

DISCUSSION

Characteristics of types of information attacks in social networks. Information threat is a set of conditions and factors that create a potential or real threat of information security violations.

It is necessary to highlight the characteristics of the protection against the spread of information attacks and their classification in advance.

Information attacks on social networks can be classified according to several main criteria:

- objects of influence;
- purpose of influence;
- methods of carrying out attacks;
- sources of exposure;

Objects of influence:

Social network users;

Developers, administration and technical staff;

Equipment (servers, workstations, network equipment, communication channels);

Software.

Impact goals:

Technical and informational (software impact):

- malfunction of equipment;

- limiting the availability of the communication channel;
- Violation of data integrity and relevance. Change or remove information;

It is possible to put an isomorphism in the assumption-based methods of exchanging information on threats. Some biological models can be adapted for use in social networks.

ANALYSIS AND RESULTS

Mathematical models that use biological approaches to describe the process of spreading destructive information are differential equations and based on reflecting the epidemic process as a change in the number of objects in one of several discrete cases.

Distribution of information attacks based on the SI mathematical model (Susceptible- Infected)

One example is the mathematical model SI (Susceptible-Infected), which is characterized by the existence of two states of objects: infected (I) and uninfected (S).

The general structure of a social network based on the SI model can be:

$$\boldsymbol{N = S(t) + I(t)}$$

here:

$\boldsymbol{N}$ is the total number of users in the social network;

$\boldsymbol{S(t)}$ is the number of users who are not familiar with the malicious information;

$\mathbf{I}(t)$ is the number of users who positively received the malicious information and contributed to its spread in the social network.

Obviously, this model does not account for the fact that a certain proportion of users who have not previously been exposed to destructive information $S(t)$ will turn out to be immune to destructive information. In this case, the SI model is converted to the SIR (SI-Recovered) model, taking into account the user mmunity.

Distribution of information attacks based on SIR (Susceptible-Infected-Recovered) mathematical model

The SIR (Susceptible-Infected-Recovered) mathematical model has three different object states: uninfected (S), infected (I) and disinfected objects with immunity (R).

The general structure of a social network based on the SIR model can be as follows:

Expressed using the expression $\boldsymbol{N = S(t) + I(t) + R(t).}$ here:

$\boldsymbol{N}$ is the total number of users in the social network;

$\boldsymbol{S(t)}$ is the number of users who are not familiar with the malicious information;

$\boldsymbol{I(t)}$ is the number of users who positively received malicious information and contributed to its spread in the social network;

$\boldsymbol{R(t)}$ is the number of non-users.

If the action (notification) occurs instantaneously, the statement is true, but if it occurs over a period of time, then the number of N due to new users increases and, for example, decreases in N, accounts are blocked or deleted.

Distribution of information attacks based on mathematical model and SIRS (Susceptible-Infected-Recovered-Susceptible)

One of the disadvantages of the SIR model is that previously unresponsive users may be exposed to disruptive information in the future. This drawback is overcome by converting the SIR model into a SIRS

(susceptible-infected-recovery-susceptible) model, where a previously unresponsive user becomes susceptible after some time.

Introducing an additional type of control object and taking into account new possible discrete states also allows to increase the accuracy of the mathematical model, but in real conditions it is not possible to guarantee the transition from one state to another and back. It should be remembered that information warfare tools cannot work immediately, but only after a certain period of time [5]. In the case of strong information conflicts, the user may switch from one state to another several times or ignore destructive information at all. These factors are not taken into account in the SIRS model, which reduces the scope of this model. The advantage of this model is the simplicity of implementation, but the application of this model in real conditions is limited at the stage of negative impact on information.

CONCLUSION

It can be concluded that the use of biological approaches in mathematical models describing the spread of information threats allows to identify characteristic features and obtain a mathematical estimate of the spread. The SIR model most accurately describes the process of malicious information dissemination and can be used to predict the spread of information threats in some cases.

List of used literature:

1. Alimov R.Kh., Khodiyev B. Yu. and others. Information systems and technology in the national economy gyals. Tashkent. "Sharq", 2004.
2. Aripov M., Begalov B. and others. Information Technology. For higher educational institutions study guide. Tashkent-Noshir-2009.
3. Fundamentals of Library and Informational science‖, by ABDUWAHAB OLANREWAJU ISSA, Ph.D in 2013, pages – 133.
4. Harris, M.H. History of Libraries in the Western World, 4th ed. (Scarecrow, 2011)

Internet resources:

5. http://en.wikipedia.org/wiki/Library_science
6. http://WWW.rocket-library.com/)
7. http://en.wikipedia.org/wiki/List_of_libraries